COPY


## ABSTRACT

An architecture for secure access of machines inside an organization from a remote machine that is connected to the Internet uses two dedicated computers outside the firewall. To ensure security the system makes use of biometrics features and a one-time password mechanism on top of secure socket layer (SSL) to authenticate a user. The system also provides three layers of security levels for transmission. In the first layer, establishes an SSL connection, the second layer periodically asks for a one-time password (OTP), and the third layer uses any kind of conventional encryption. The system also uses a mechanism for secure file accesses within the organization based on the security privileges assigned to various users. The files to be accessed from the server are categorized depending on their access privileges and encrypted using a key assigned to each category. The users are also assigned various access privileges to these files. Two software modules are proposed, one resides on the server and the other residing at the user's machine. Based on the user's access privileges, the server side software module sends the requested file in an encrypted form along with the key to decrypt that file – this key is encrypted by the user's strong password. The software module at the user's end then uses his strong password to decrypt the encryption key of the file, and then uses this key to decrypt the file.